

日本国特許庁
JAPAN PATENT OFFICE

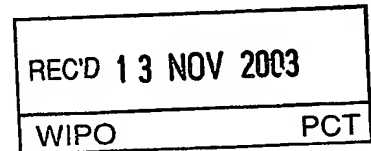
25.09.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年 9月30日
Date of Application:

出願番号 特願2002-285168
Application Number:
[ST. 10/C]: [JP2002-285168]



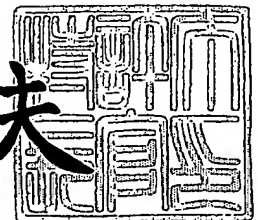
出願人 FDK株式会社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年10月30日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 IP02507

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 7/58

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 エフ・ディー・ケ
イ株式会社内

【氏名】 山本 博康

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 エフ・ディー・ケ
イ株式会社内

【氏名】 アナンダ ビターナゲ

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 エフ・ディー・ケ
イ株式会社内

【氏名】 清水 隆邦

【発明者】

【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 エフ・ディー・ケ
イ株式会社内

【氏名】 藤田 香

【特許出願人】

【識別番号】 000237721

【氏名又は名称】 エフ・ディー・ケイ株式会社

【代理人】

【識別番号】 100067046

【弁理士】

【氏名又は名称】 尾股 行雄

【電話番号】 03-3543-0036

【選任した代理人】

【識別番号】 100096862

【弁理士】

【氏名又は名称】 清水 千春

【電話番号】 03-3543-0036

【手数料の表示】

【予納台帳番号】 008800

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 物理乱数の一様化手法

【特許請求の範囲】

【請求項 1】 複数の物理乱数を乱数保持装置（2）に入力して保持し、この乱数保持装置に保持された物理乱数をその一部に基づいてランダムに選択して出力することを特徴とする物理乱数の一様化手法。

【請求項 2】 複数の物理乱数を乱数保持装置（2）に入力して保持し、この乱数保持装置に保持された物理乱数をその一部に基づいてランダムに選択して出力する操作を 1 サイクルとし、

この操作を 2 サイクル以上繰り返して物理乱数を多段に一様化することを特徴とする物理乱数の一様化手法。

【請求項 3】 乱数保持装置としてシフトレジスタ（2）を用いたことを特徴とする請求項 1 または請求項 2 に記載の物理乱数の一様化手法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、偏りのある物理乱数を簡単に一様化することが可能な物理乱数の一様化手法に関するものである。

【0002】

【従来の技術】

一般に乱数には、計算によって決定論的に生成される擬似乱数と、自然界の物理現象を利用して生成される物理乱数とがある。後者（物理乱数）は真の意味でランダムな現象を基に生成されるので、理想的な乱数となる資質があるものの、実際に物理乱数を生成する場合、途中過程で様々な誤差要因が介在するため、必ずしも理想的な乱数が出力されとは限らず、偏りのある乱数が出てきてしまう恐れもある。この誤差要因としては、デジタル化の際に基準となるクロックの幅や、ノイズを利用する場合に余計なノイズが混入することなどが挙げられる。

【0003】

従来、こうした物理乱数の偏りを改善する手法、すなわち物理乱数の一様化手

法としては、2つの2進乱数を用いて乱数の偏りを改善するノイマンコレクター（例えば、非特許文献1参照）や、ノイズに基づいて発生させた物理乱数を擬似乱数と合成することで物理乱数の偏りを改善する手法（以下、乱数合成法と称する。）が提案されていた（例えば、特許文献1参照）。

【0004】

【特許文献1】特開2001-344094号公報（段落〔0014〕〔0018〕の欄、図1）

【非特許文献1】Benjamin Jun and Paul Kocher著、"The Intel Random Number Generator"、CRYPTOGRAPHY RESEARCH、1999年4月22日発表（第4頁、4.3.Digital Post-Processing）

【0005】

【発明が解決しようとする課題】

しかし、ノイマンコレクターでは、1ビットの乱数を出力するのに2ビットの乱数を必要とする上に、その2ビットの組合せによっては乱数を出力しない場合もあるので、乱数の発生速度が落ちてしまう欠点があった。

【0006】

また、乱数合成法では、擬似乱数がわかれば、基になる物理乱数を出力から取り出せるようになるため、乱数の偏りが他人に知られてしまい、保安性に欠けるという不都合があった。

【0007】

本発明は、このような事情に鑑み、乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供することを目的とする。

【0008】

【課題を解決するための手段】

まず、本発明のうち請求項1に係る発明は、複数の物理乱数を乱数保持装置（2）に入力して保持し、この乱数保持装置に保持された物理乱数をその一部に基づいてランダムに選択して出力するようにして構成される。こうした構成を採用することにより、乱数保持装置に入力された物理乱数は、たとえそれが偏りを持っていても一様化されて出力され、乱数を出力しない場合や乱数の偏りが他人に

知られてしまう事態が起きないように作用する。

【0009】

また、本発明のうち請求項2に係る発明は、複数の物理乱数を乱数保持装置（2）に入力して保持し、この乱数保持装置に保持された物理乱数をその一部に基づいてランダムに選択して出力する操作を1サイクルとし、この操作を2サイクル以上繰り返して物理乱数を多段に一様化するようにして構成される。かかる構成により、物理乱数の一様化が一層促進されるように作用する。

【0010】

さらに、本発明のうち請求項3に係る発明は、上記乱数保持装置としてシフトレジスタ（2）を用いて構成される。

【0011】

なお、括弧内の符号は図面において対応する要素を表す便宜的なものであり、したがって、本発明は図面上の記載に限定拘束されるものではない。このことは「特許請求の範囲」の欄についても同様である。

【0012】

【発明の実施の形態】

以下、本発明の実施形態を図面に基づいて説明する。

図1は本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の二例を示す回路図、

図2は本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の別の二例を示す回路図、

図3は本発明に係る物理乱数の一様化手法が適用される乱数一様化回路のさらに別の二例を示す回路図である。

【0013】

まず、図1（a）に示す乱数一様化回路1では、シフトレジスタ2とセレクタ3とを具備しており、シフトレジスタ2のデータ端子Dには2進乱数（「0」または「1」）が順次入力され、シフトレジスタ2のクロック端子CLKに入力される基準パルス信号が立ち上がるごとに、これらの2進乱数が順に出力Q00～Q134にシフトされていく。そして、シフトレジスタ2の出力Q00～Q12

7の128ビットの乱数はそれぞれセクタ3のデータ端子D00～D127に
入力され、シフトレジスタ2の出力Q128～Q134の7ビットの乱数はそれ
ぞれセクタ3のアドレスAD0～AD6に入力される。

【0014】

その後、セクタ3では、アドレスAD0～AD6に入力された7ビットのア
ドレス値に応じて、データ端子D00～D127に入力された128ビットの乱
数から1ビットが選択され、出力端子OUTから出力される。例えば、アドレ
スAD0～AD6にそれぞれ「1」「0」「0」「0」「0」「0」「0」が入力
されたときは、データ端子D00に入力された乱数が出力端子OUTから出力さ
れる。また、アドレスAD0～AD6にそれぞれ「1」「0」「1」「0」「0」
「0」「0」が入力されたときは、データ端子D04に入力された乱数が出力
端子OUTから出力される。

【0015】

このように、シフトレジスタ2のデータ端子Dに順次入力される2進乱数は、
その一部がアドレスとなって自分自身をランダムに選び出すので、この2進乱数
が偏りを持っていても、この乱数一様化回路1で一様化されて出力されることにな
る。しかも、従来のノイマンコレクターと異なり、1ビットの乱数を出力する
のに複数ビットの乱数を必要とすることもなく、乱数を出力しない場合もないた
め、乱数の発生速度を維持することができる。また、従来の乱数合成法と違って
、乱数の偏りが他人に知られてしまう事態が生じないので、保安性を確保するこ
とができる。

【0016】

また、図1(b)に示す乱数一様化回路1は、シフトレジスタ2からの乱数出
力を選択するビット数を6ビットに減らしたことで、排他的論理和(XOR)回
路を追加したことを除き、図1(a)に示す乱数一様化回路1と同様である。す
なわち、図1(b)に示す乱数一様化回路1では、シフトレジスタ2とセクタ
3とを具備しており、セクタ3の出力と2進乱数(「0」または「1」)とを
入力とする排他的論理和回路の出力が順次シフトレジスタ2のデータ端子Dに入
力され、シフトレジスタ2のクロック端子CLKに入力される基準パルス信号が

立ち上がるごとに、出力Q00～Q69に順にシフトされていく。そして、シフトレジスタ2の出力Q00～Q63の64ビットの乱数はそれぞれセクタ3のデータ端子D00～D63に入力され、シフトレジスタ2の出力Q64～Q69の6ビットの乱数はそれぞれセクタ3のアドレスAD0～AD5に入力される。その後、セクタ3では、アドレスAD0～AD5に入力された6ビットのアドレス値に応じて、データ端子D00～D63に入力された64ビットの乱数から1ビットが選択され、出力端子OUTから出力される。

【0017】

この場合も、シフトレジスタ2のデータ端子Dに順次入力される2進乱数は、その一部がアドレスとなって自分自身をランダムに選び出すので、この2進乱数が偏りを持っていても、この乱数一様化回路1で一様化されて出力されることになり、乱数の発生速度を維持すると同時に、保安性を確保することができる。

【0018】

このことを確認するため、この乱数一様化回路1から出力された乱数の一様性を乱数検定規格FIPS140-2に準拠して評価した。その結果を表1および表2に示す。なお、表1中の数値は元データを表し、表2中の数値は検定結果データを表す。ここで、表1、2中の「Mono」、「Poker」、「Runs」および「Long Run」は乱数検定の種類を表しており、それぞれ乱数検定規格FIPS140-2の「Monobit Test」、「Porker Test」、「Runs Test」および「Long Run Test」に対応している。また、結果は50回を1セットとして表示しており、数値は50回の検定中で不合格になった回数を表している。

【表1】

セットNo.	Mono	Poker	Runs	LongRun
1	0	0	1	0
2	0	0	0	0
3	0	0	1	0
4	0	0	1	0
5	0	0	1	0
6	0	0	2	0
7	0	0	0	0
8	0	0	0	0
9	0	0	1	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	1	0
15	0	0	0	0
16	0	0	1	0
17	0	0	1	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	1	1
22	0	0	1	0
23	0	0	1	0
24	0	0	0	0
25	0	0	0	0
26	0	0	1	0
27	0	0	0	0
28	0	0	0	0
29	0	0	1	0
30	1	0	0	0
31	0	0	0	1
32	0	0	1	0
33	0	0	0	0
34	0	0	0	0
35	0	0	0	1
36	0	0	1	0
37	0	0	1	0
38	0	0	0	0
39	0	0	0	0
40	0	0	0	0
41	0	0	0	0
42	0	0	0	0
43	0	0	1	0
44	0	0	0	0
45	0	0	0	0
46	0	0	2	0
47	0	0	0	0
48	0	0	1	0
49	0	0	0	0
50	0	0	0	0

【表 2】

セット No.	Mono	Poker	Runs	LongRun
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	1	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0
27	0	0	0	0
28	0	0	0	0
29	0	0	0	0
30	0	0	0	0
31	0	0	0	0
32	0	0	0	0
33	0	0	0	0
34	0	0	0	0
35	0	0	0	0
36	0	0	0	0
37	0	0	0	0
38	0	0	0	0
39	0	0	0	0
40	0	0	0	0
41	0	0	1	0
42	0	0	0	0
43	0	0	0	0
44	0	0	0	0
45	0	0	0	0
46	0	0	0	0
47	0	0	0	0
48	1	0	0	0
49	0	0	0	0
50	0	0	0	0

【0019】

表 1、2 から明らかなように、4 種類すべての乱数検定（「Mono」、「Poker」、「Runs」および「LongRun」）において、セットNo. 1 ～ 50 のほとんど全部が合格値となり、上述した効果が確認された。

【0020】

一方、図 2（a）に示す乱数一様化回路 1 は、シフトレジスタ 2 からの乱数出力を選択するビット数を 15 ビットに増やしたことで、セレクタ 3 と同様な働きをするものとして論理積（AND）回路と排他的論理和（XOR）回路との組み合わせを代用したことを除き、図 1（a）に示す乱数一様化回路 1 と同様である。すなわち、図 2（a）に示す乱数一様化回路 1 ではシフトレジスタ 2 を具備しており、シフトレジスタ 2 のデータ端子 D には 2 進乱数（「0」または「1」）が順次入力され、シフトレジスタ 2 のクロック端子 CLK に入力される基準パルス信号が立ち上がるごとに、これらの 2 進乱数が順に出力 Q00 ～ Q30 にシフトされていく。そして、シフトレジスタ 2 の出力 Q00 ～ Q14 の 15 ビットの乱数とシフトレジスタ 2 の出力 Q16 ～ Q30 の 15 ビットの乱数とを入力とする 15 個の論理積回路の出力が、シフトレジスタ 2 の出力 Q15 とともに排他的論理和回路で順次合成されて出力される。

【0021】

このように、シフトレジスタ 2 のデータ端子 D に順次入力される 2 進乱数は、シフトレジスタ 2 内で同じビット数（15 ビット）の 2 組に分けられた後、論理積回路と排他的論理和回路でランダムに演算されるので、この 2 進乱数が偏りを持っていても、この乱数一様化回路 1 で一様化されて出力されることになる。しかも、従来のノイマンコレクターと異なり、1 ビットの乱数を出力するのに複数ビットの乱数を必要とすることもなく、乱数を出力しない場合もないため、乱数の発生速度を維持することができる。また、従来の乱数合成法と違って、乱数の偏りが他人に知られてしまう事態が生じないので、保安性を確保することができる。

【0022】

また、図 2（b）に示す乱数一様化回路 1 は、シフトレジスタ 2 からの乱数出力を選択するビット数を 7 ビットに減らしたことで、排他的論理和（XOR）回

路を追加したことを除き、図 2 (a) に示す乱数一様化回路 1 と同様である。すなわち、図 2 (b) に示す乱数一様化回路 1 ではシフトレジスタ 2 を具備しており、シフトレジスタ 2 のデータ端子 D には 2 進乱数（「0」または「1」）が順次入力され、シフトレジスタ 2 のクロック端子 CLK に入力される基準パルス信号が立ち上がるごとに、これらの 2 進乱数が順に出力 Q00～Q14 にシフトされていく。そして、シフトレジスタ 2 の出力 Q00～Q06 の 7 ビットの乱数とシフトレジスタ 2 の出力 Q08～Q14 の 7 ビットの乱数とを入力とする 7 個の論理積回路の出力が、シフトレジスタ 2 の出力 Q07 とともに排他的論理和回路で順次合成され、最後に元の 2 進乱数（生データ）と排他的論理和回路で合成されて出力される。

【0023】

この場合も、シフトレジスタ 2 のデータ端子 D に順次入力される 2 進乱数は、シフトレジスタ 2 内で同じビット数（7 ビット）の 2 組に分けられた後、論理積回路と排他的論理和回路でランダムに演算されるので、この 2 進乱数が偏りを持っていても、この乱数一様化回路 1 で一様化されて出力されることになり、乱数の発生速度を維持すると同時に、保安性を確保することができる。

【0024】

なお、上述の実施形態においては、複数の物理乱数を保持する乱数保持装置としてシフトレジスタ 2 を用いた場合について説明したが、シフトレジスタ 2 以外の乱数保持装置（例えば、フリップフロップ）を代用することもできる。

【0025】

また、上述の実施形態においては、1 個の乱数一様化回路 1 を用いて物理乱数を一様化する場合について説明したが、図 3 に示すように、図 1 や図 2 に示す乱数一様化回路 1 を 2 個以上接続して物理乱数を多段に一様化することもできる。この場合、乱数一様化回路 1 の接続方法は、図 3 (a) に示すような直列接続であっても、図 3 (b) に示すような並列接続であっても構わない。

【0026】

【発明の効果】

以上説明したように、本発明によれば、乱数保持装置（シフトレジスタ）に入

力された物理乱数は、たとえそれが偏りを持っていても一様化されて出力され、乱数を出力しない場合や乱数の偏りが他人に知られてしまう事態が起きないことから、乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供することができる。

【図面の簡単な説明】

【図 1】

本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の二例を示す回路図である。

【図 2】

本発明に係る物理乱数の一様化手法が適用される乱数一様化回路の別の二例を示す回路図である。

【図 3】

本発明に係る物理乱数の一様化手法が適用される乱数一様化回路のさらに別の二例を示す回路図である。

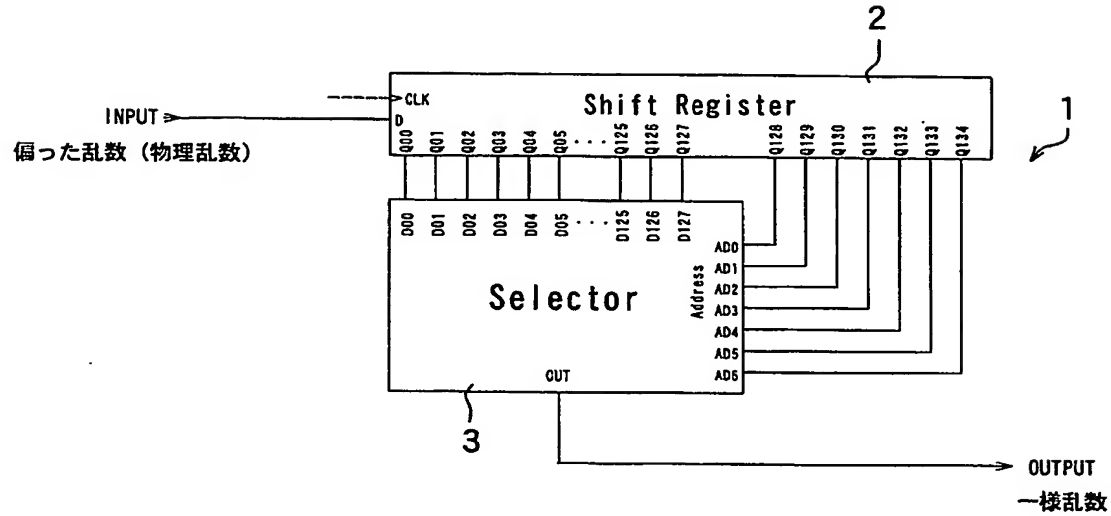
【符号の説明】

- 1 ……乱数一様化回路
- 2 ……シフトレジスタ（乱数保持装置）
- 3 ……セクタ

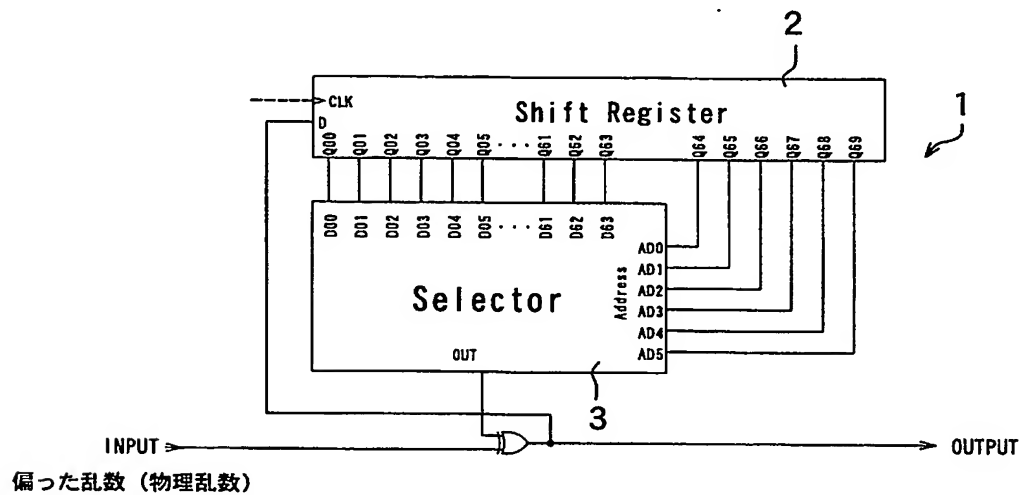
【書類名】 図面

【図 1】

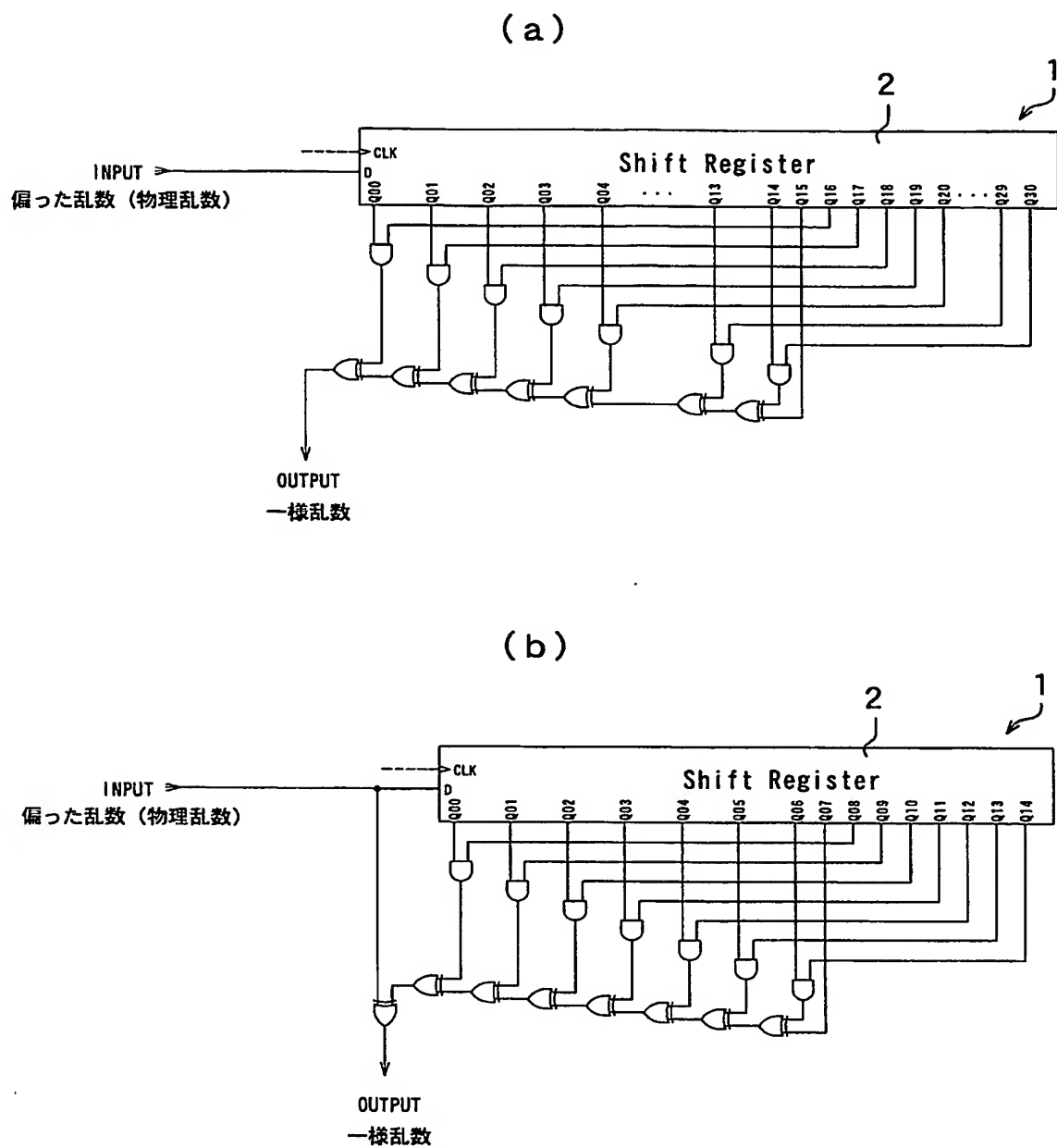
(a)



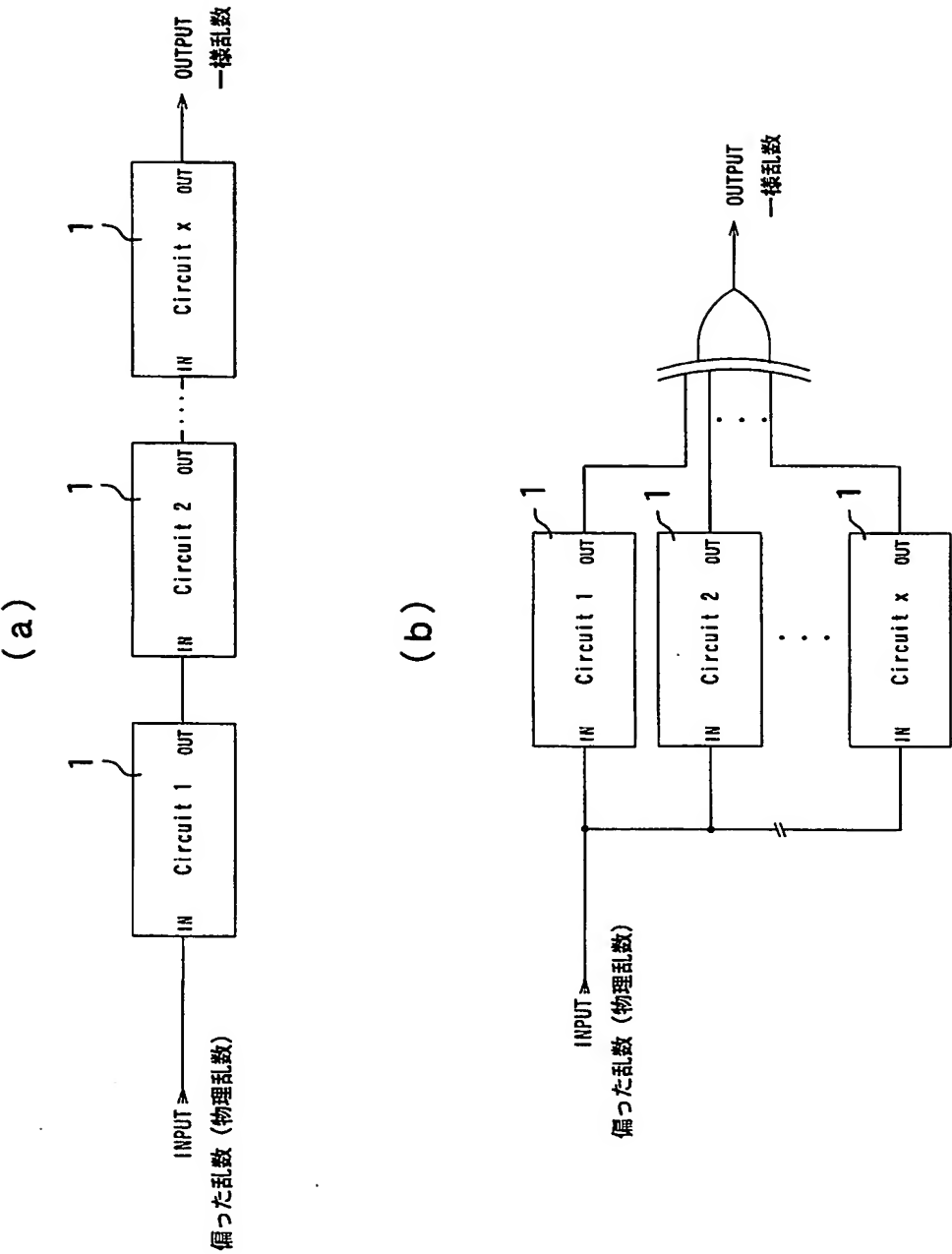
(b)



【図 2】



【図 3】



【書類名】 要約書

【要約】

【課題】 乱数の発生速度を維持すると同時に保安性をも確保することが可能な物理乱数の一様化手法を提供する。

【解決手段】 複数の物理乱数をシフトレジスタ 2 に順次入力して保持し、基準パルス信号が立ち上がるごとにシフトする。シフトレジスタ 2 に保持された物理乱数をその一部に基づいてセレクト 3 でランダムに選択して出力する。これにより、シフトレジスタ 2 に入力された物理乱数は、それが偏りを持っていても一様化されて出力され、乱数を出力しない場合や乱数の偏りが他人に知られる事態が起きない。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2002-285168
受付番号	50201463033
書類名	特許願
担当官	第七担当上席 0096
作成日	平成14年10月 1日

<認定情報・付加情報>

【提出日】	平成14年 9月30日
-------	-------------

次頁無

特願 2 0 0 2 - 2 8 5 1 6 8

出 願 人 履 歴 情 報

識別番号

[0 0 0 2 3 7 7 2 1]

- | | |
|----------|--------------------------|
| 1. 変更年月日 | 2 0 0 1 年 1 月 1 6 日 |
| [変更理由] | 名称変更 |
| 住 所 | 東京都港区新橋 5 丁目 3 6 番 1 1 号 |
| 氏 名 | エフ・ディー・ケイ株式会社 |
| 2. 変更年月日 | 2 0 0 3 年 8 月 1 3 日 |
| [変更理由] | 名称変更 |
| 住 所 | 東京都港区新橋 5 丁目 3 6 番 1 1 号 |
| 氏 名 | F D K 株式会社 |